



## Municipal Corporate ICT Governance Framework Policy

Date Approved	Version	Resolution Number
31 May 2023	4	

*The Information Communication Technology Manager*

*Senqu Local Municipality*

*19 Murray Street*

*Lady Grey*

*Telephone (051) 603 1300*

*Facsimile (051) 603 0445*

*Website: [www.senqu.gov.za](http://www.senqu.gov.za)*

Resolution:

Approved:

**Municipal Corporate ICT Governance Framework Policy**

Information and Communications Technology (ICT) Governance has been described as the effective and efficient management of ICT resources to facilitate the achievement of organisational goals and objectives. ICT does not exist for its own sake within an organisation; ICT is there to make sure that organisations achieve sustainable success through the use of their ICT. ICT is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's ICT (the infrastructure as well as the capabilities and organisation that is established to support ICT) sustains and extends the organisation's strategies and objectives.

<b>Full Title</b>	Municipal Corporate ICT Governance Framework Policy
<b>Short Title</b>	ICT Governance
<b>Author(s)</b>	Mr R Johl & Mrs M Oertel
<b>Reviewer(s)</b>	Mr LE Booie and Mr K Fourie

**Table of Contents**

1.	Version Control.....	3
2.	Definitions.....	4
3.	Introduction.....	6
4.	Purpose.....	6
5.	Scope/Audience.....	7
6.	Role of the ICT business unit.....	7
7.	Municipal Corporate ICT Governance Framework Policy Objectives.....	8
8.	Benefits of Good Governance of ICT.....	9
9.	Legislative Framework.....	11
10.	Corporate Governance of ICT Good Practices and Standards.....	11
11.	Layered Approach to Corporate Governance of ICT in Municipalities.....	12
12.	ICT Governance Framework Components.....	13
13.	Policy Violations.....	41
14.	Policy Review.....	41
15.	Publishing the policy.....	41
16.	Senqu Municipality Approval and Sign-Off.....	42
	Appendix A: ICT Governance Processes.....	43

## 1. Version Control

<b>Full Title</b>	<b>Senqu Municipality-Municipal Corporate ICT Governance Framework Policy</b>
<b>Short Title</b>	MCGICT Policy
<b>Author(s)</b>	Mr N Suleman
<b>Version</b>	0.1

<b>Authors</b>	Mr N Suleman (PWC) & Ms. Magdalena Oertel (Senqu)
<b>Version</b>	01
<b>Authorised By</b>	Council
<b>Version Date</b>	30 June 2016
<b>Effective Date</b>	1 July 2016

<b>Revised</b>	Ms. Magdalena Oertel (Senqu Municipality)
<b>Version</b>	02
<b>Authorised By</b>	Council
<b>Version Date</b>	28 July 2017
<b>Effective Date</b>	1 July 2017

<b>Revised</b>	Mr Luzuko Booï and Mr K Fourie (Senqu Municipality)
<b>Version</b>	03
<b>Authorised By</b>	Council
<b>Version Date</b>	26 May 2021
<b>Effective Date</b>	1 July 2021

## 2. Definitions

Term	Meaning
<b>ACCESS CONTROL</b>	The process that limits and controls access to resources of a computer system; a logical or physical control designed to protect against unauthorized entry or use
<b>AG</b>	Auditor-General of South Africa
<b>ANTIVIRUS SOFTWARE</b>	Applications that detect, prevent and possibly remove all known viruses from files located in a microcomputer hard drive
<b>APPLICATION RECOVERY</b>	The component of Disaster Recovery that deals specifically with the restoration of business system software and data, after the processing platform has been restored or replaced.
<b>AUDIT RISK</b>	The risk that information or financial reports may contain material errors or that the IS auditor may not detect an error that has occurred; also used to describe the level of risk that an auditor is prepared to accept during an audit engagement
<b>BACKUP</b>	Files, equipment, data and procedures available for use in the event of a failure or loss,
<b>BUSINESS CONTINUITY PLAN (BCP)</b>	Process of developing advanced arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change.
<b>CFO</b>	Chief Financial Officer
<b>CGICTPF</b>	Corporate Governance of ICT Policy Framework
<b>CIO</b>	Chief Information Officer
<b>COBICT 5</b>	Control Objectives of Information and related Technology
<b>COMMAND CENTRE</b>	A separate facility equipped with adequate communications equipment, from which initial recovery efforts are manned and media-business communications are maintained. The management team uses this facility temporarily to begin coordinating the recovery process until the alternate sites are functional
<b>COGTA</b>	Department of Cooperative Governance and Traditional Affairs
<b>DISASTER</b>	A sudden, unplanned catastrophic event causing great damage or loss. Any event that causes an organisation to be unable to provide critical business functions for a pre-determined period of time.
<b>DISASTER RECOVERY PLAN</b>	The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business disruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.
<b>DISASTER TOLERANCE</b>	Disaster tolerance is the time gap during which the business can accept the non-availability of ICT facilities.
<b>DPSA</b>	Department of Public Service and Administration
<b>E-MAIL / INTERPERSONAL MESSAGING</b>	An individual using a terminal, PC or an application can access a network to send an unstructured message to another individual or group of people.
<b>EXCO</b>	Executive Committee

<b>FIREWALL</b>	A device that enforces security policies for traffic traversing to and from different network segments. A firewall no longer only protects a Municipality from the Internet, but also protects sensitive segments within organizations.
<b>GEOGRAPHICAL INFORMATION SYSTEM (GIS)</b>	A tool used to integrate, convert, handle, analyze and produce information regarding the surface of the earth.
<b>GICTF</b>	Governance of Information and Communication Technology Framework
<b>GICTO</b>	Government Information Technology Officer
<b>HELP DESK</b>	A service offered via phone/Internet by an organization to its clients or employees, which provides information, assistance, and troubleshooting advice regarding software, hardware, or networks.
<b>ICT</b>	Information and Communication Technology
<b>ICT GOVERNANCE FRAMEWORK</b>	A model that integrates a set of guidelines, policies and methods that represent the organizational approach to the ICT governance.
<b>IM</b>	Information Management
<b>ISACA</b>	Information Systems Audit and Control Association
<b>ISMS</b>	Information Security Management System
<b>ISO</b>	International Organisation for Standardisation
<b>ISO/IEC</b>	International Organisation for Standardisation (ISO) and the International Electro technical Commission (IEC)
<b>ISO/IEC 27002</b>	International Standard on Corporate Governance of ICT (ISO/IEC WD 27002: 2013)
<b>ICTGICTM</b>	ICT Governance Institute
<b>ITIL</b>	The Information Technology Infrastructure Library
<b>KING V</b>	The KING V Report and Code on Governance for South Africa
<b>LOCAL AREA NETWORK (LAN)</b>	Communications networks that serve several users within a specified geographical area.
<b>M&amp;E</b>	Monitoring and Evaluation
<b>MFMA</b>	Municipal Finance Management Amendment Act 56, 2003
<b>MCICTGFP</b>	Municipal Corporate ICT Governance Framework Policy
<b>MM</b>	Municipal Manager
<b>THE MUNICIPALITY</b>	Senqu Local Municipality
<b>OFFSICTE STORAGE</b>	A storage facility located away from the building housing the primary information processing facility (IPF), used for storage of computer media such as offline backup data and storage files
<b>OLA</b>	Organisational Level Agreement
<b>PRINCE2</b>	PRojects IN Controlled Environments (Project Management Frameworks)
<b>PSCGICTPF</b>	Public Service Corporate ICT Governance Policy Framework
<b>RFI</b>	Request for Information
<b>RFP</b>	Request for Proposal
<b>SALGA</b>	South African Local Government Association
<b>SDBIP</b>	Service Delivery Budget Implementation Plan
<b>SERVICE PROVIDER</b>	Supplier of services to the municipality
<b>SLA</b>	Service Level Agreement
<b>UPS</b>	Uninterrupted Power Supply is a device that provides battery backup when the electrical power fails or drops to an unacceptable voltage level

### 3. Introduction

ICT Governance is defined as a subset discipline of Corporate Governance focused on information technology (ICT) systems and their performance and risk management.

ICT Governance can be further defined as the process by which ICT decisions are made and incorporate how decisions are made, who makes decisions, who is held accountable and how the results of the decisions are measured and monitored.

ICT Governance is the responsibility of Senior Management and consists of the leadership, Municipal structures and processes that ensure that the Municipality's ICT business unit sustains and extends the Municipality's strategies and objectives.

#### 3.1 Corporate Governance in Municipalities:

Corporate governance is a vehicle through which value is created within a municipal context. Value creation means realising benefits while optimising resources and risks. This value creation takes place within a governance system that is established by the municipal policy. A governance system refers to all the means and mechanisms that enable the Municipality's Council and Management team to have a structured and organised process.

#### 3.2 Corporate Governance of ICT in Municipalities:

The Corporate Governance of ICT is an integral part of the corporate governance system in municipalities. The Corporate Governance of ICT involves evaluating, directing and monitoring the alignment of the ICT strategy with the Municipality's IDP and related strategies. The Corporate Governance of ICT also involves the monitoring of ICT service delivery to ensure a culture of continuous ICT service improvement exists at the Municipality. The Corporate Governance of ICT includes determining ICT strategic goals and plans for ICT service delivery as determined by the Service Delivery and Budget Implementation Plan (SDBIP) objectives of the Municipality.

### 4. Purpose

The purpose of this policy is to institutionalise the Corporate Governance of ICT as an integral part of corporate governance within the Municipality in a uniform and coordinated manner. This policy provides the Municipal Council and Management within a municipality with a set of principles and practices that must be complied with, together with an implementation approach to be utilised for implementation in order to institutionalise the Corporate Governance of ICT.

## The Governance and Situational Context

The Municipality has identified the need to replace its existing governance framework which focused on KING V with a framework which incorporates KING V, COBICT 5 and ICTIL V4 which will better assist in shaping the direction the municipality wishes to take. Understanding the importance of a governance framework is thus an important step in the process of building a competitive and world-class industrial development zone.

### 4.1. ICT Governance in the Municipality

ICT governance is a framework that supports the effective and efficient management of information resources (e.g., people, funding and information) to facilitate the achievement of strategic objectives. The focus is on the measurement and management of ICT performance to ensure that the risks and costs associated with ICT are appropriately controlled.

Governance creates an environment for proper control between the business and the ICT unit and how the municipality views governance is an important part of the implementation process of the suggested framework.

The formulation of the committees and their roles and responsibilities which will govern ICT, should have in place terms of reference for all members to adhere to and comply with in order for governance to be effective. The various committees should take key decisions that will help propel the municipality towards its strategic objectives.

## 5. Scope/Audience

This Policy has been developed to guide and assist the Municipality to be aligned with the Corporate Governance of ICT best practice frameworks. This Policy therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective Corporate Governance of ICT.

## 6. Role of the ICT business unit

The Municipal Manager will appoint a suitably qualified and experienced ICT Manager. The ICT Manager has the responsibility to manage the ICT business unit which will serve Senqu Municipality.

The objectives of the ICT business unit are as follows:



- 6.1 To ensure that the ICT Strategy is aligned to the Municipality's strategy. Opportunities to improve the use of ICT within Senqu Municipality are identified and exploited. That optimal investment is made in ICT, costs are managed and the return on investment is measured.
- 6.2 Synergies between ICT initiatives are enabled, and ICT choices are in the best interest of the Municipality as a whole and not only those of individual business units.
- 6.3 ICT services are sourced optimally and legitimately.
- 6.4 ICT risks are identified and adequately addressed. Assurance is obtained to ensure that an ICT control framework is in place to address ICT risks.
- 6.5 Information, ICT assets and intellectual property contained in ICT systems are protected and effectively managed and used.
- 6.6 ICT has adequate business resilience arrangements in place for disaster recovery.
- 6.7 Information management is a joint ICT and business responsibility.
- 6.8 ICT use conforms to ICT related laws and related rules, codes and standards.
- 6.9 ICT use is sustainable with respect to the environment.

## **7. Municipal Corporate ICT Governance Framework Policy Objectives**

The objective of this Corporate Governance of ICT Policy for the Municipality seeks to achieve the following:

- 7.1 Institutionalising a Corporate Governance of ICT Policy that is consistent with the Corporate Governance Framework of the Municipality.
- 7.2 Aligning the ICT strategic goals and objectives with the Municipality's strategic goals and objectives.
- 7.3 Ensuring that optimum Municipal value is realised from ICT-related investment, services and assets.
- 7.4 Ensuring that Municipal ICT-related risks do not exceed the Municipality's risk appetite and risk tolerance.
- 7.5 Ensuring that ICT-related resource needs are met in an optimal manner by providing the organisational structure, capacity and capability.
- 7.6 Ensuring that communication with stakeholders is transparent, relevant and timely.
- 7.7 Ensuring transparency of performance and conformance and driving the achievement of strategic goals through monitoring and evaluation.
- 7.8 ICT should be aligned with the performance and sustainability objectives of the Municipality.
- 7.9 To support effective and efficient management of ICT resources to facilitate the achievement of a Municipality's objectives.
- 7.10 To put relevant structures, processes, and mechanism to enable ICT to deliver value to the Municipality and mitigate ICT risks.
- 7.11 To facilitate and enhance the Municipality's ability to reach its objectives by making the most appropriate decisions about incorporating ICT into its operations, programmes and services on a secure and sustainable basis (blue from sample)

## 8. Benefits of Good Governance of ICT

When Corporate Governance of ICT is effectively implemented and maintained, the following benefits will be realised:

- 8.1 Establishment of ICT as a strategic enabler in the Municipality.
- 8.2 Improved achievement of municipal integrated development plans.
- 8.3 Improved effective service delivery through ICT-enabled access to municipal information and services.
- 8.4 Improved ICT enablement of the Municipality.
- 8.5 Improved delivery of ICT service quality.
- 8.6 Improved stakeholder communication.
- 8.7 Improved trust between the municipality and the community through the use of ICT.
- 8.8 Lower costs for ICT functions and ICT dependent functions.
- 8.9 Increased alignment of ICT investment towards municipal integrated development plans.
- 8.10 Improved return on ICT investments.
- 8.11 ICT risks managed in line with the ICT priorities and risk appetite of the Municipality.
- 8.12 Appropriate security measures to protect both the Municipality and its employee's information.
- 8.13 Improved management of municipal-related ICT projects.
- 8.14 Improved management of information as ICT is prioritised on the same level as other resources in the Municipality.
- 8.15 ICT pro-actively recognises potential efficiencies and guides the Municipality in timeous adoption of appropriate technology coupled with ICT ability and agility to changing circumstances.
- 8.16 Improved ICT ability and agility to adapt to changing circumstances.
- 8.17 ICT executed in line with legislative and regulatory requirements.

The four key process areas that drive sound ICT Governance is the enhanced ability to direct, manage, operate and control the municipality as outlined below:

- **Direct:**
  - The governance structures in ensuring that the developed plans are kept in focus and that a conscious effort is made in reaching municipality strategic goals and objectives
  - Risks are more accurately assessed and monitored thus the risks that are inherent in the municipality such as unsatisfied tenants will be mitigated
- **Manage:**
  - The ability to monitor ROI and manage the process of maximising the use of ICT investment
  - A more accurate analysis of current conditions and development of tactics to improve the current conditions.
  - Risk management is required to mitigate the risks that have been identified.
- **Operate:**

- Development of reporting tools and their implementation.
- Mitigate risk factors on an operational level
- Execute disaster recovery plan
- **Control:**
- Enhance reporting and transparency.
- Information security and integrity

## 9. Legislative Framework

The Municipality must be aware of and comply with the legislative landscape applicable to its environment. This includes the following:

- Municipal Systems Act, Act 32, of 2000,
- Public Administration Management Act, Act 11 of 2014.
- Local Government: Municipal Finance Management Act, Act 56 of 2003.
- Constitution of The Republic of South Africa No. 108 of 1996
- Copyrights Act, Act 98 of 1978
- Electronic Communications and Transactions Act, Act 25 of 2002
- Municipal Structures Acts, Act 117, of 1998
- Municipal Systems Acts, Act 32, of 2000
- Municipal Finance Management Act, Act 56 of 2003
- Minimum Information Security Standards, as approved by Cabinet in 1996
- National Archives and Records Service of South Africa Act, Act 43 of 1996
- Promotion of Access to Information Act, Act 2 of 2000
- Protection of Personal Information Act, Act 4 of 2013
- Regulation of Interception of Communications Act, Act 70 of 2002
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005

This policy has been developed with the above-mentioned legislations and regulations considered.

## 10. Corporate Governance of ICT Good Practices and Standards

In recognition of the importance of ICT Governance, a number of internationally recognised frameworks and standards will be adopted to provide context for the institutionalisation of the governance of ICT.

- 10.1 **The KING V Code:** The most commonly accepted Corporate Governance Framework in South Africa is also valid for municipalities. It was used to inform the Governance of ICT principles and practices and to establish the relationship between Corporate Governance of and Governance of ICT.
- 10.2 **ISO/IEC 27002:** Internationally accepted as the standard for Corporate Governance of ICT; ICT provides governance principles and a model for the effective, efficient, and acceptable use of ICT within the Municipality.

10.3 **Municipal Corporate ICT Governance Framework Policy:** The purpose of the Municipal Corporate Governance ICT Policy is to institutionalise the Corporate Governance of ICT as an integral part of corporate governance within municipalities. This Municipal Corporate Governance ICT Policy provides the Municipal Council and Management within a municipality with a set of principles and practices that must be complied with, together with an implementation approach to be utilised for implementation of ICT Governance within Municipalities.

10.4 **Other** internationally accepted process frameworks for implementing Governance of ICT.

## **11. Layered Approach to Corporate Governance of ICT in Municipalities**

11.1 Corporate Governance of ICT encompasses two levels of decision-making, authority and accountability to satisfy the expectations of all stakeholders. These levels are:

11.1.1 Facilitating the achievement of the Municipality's strategic goals (Corporate Governance of ICT).

11.1.2 The efficient and effective management of ICT service delivery (Operational Governance of ICT).

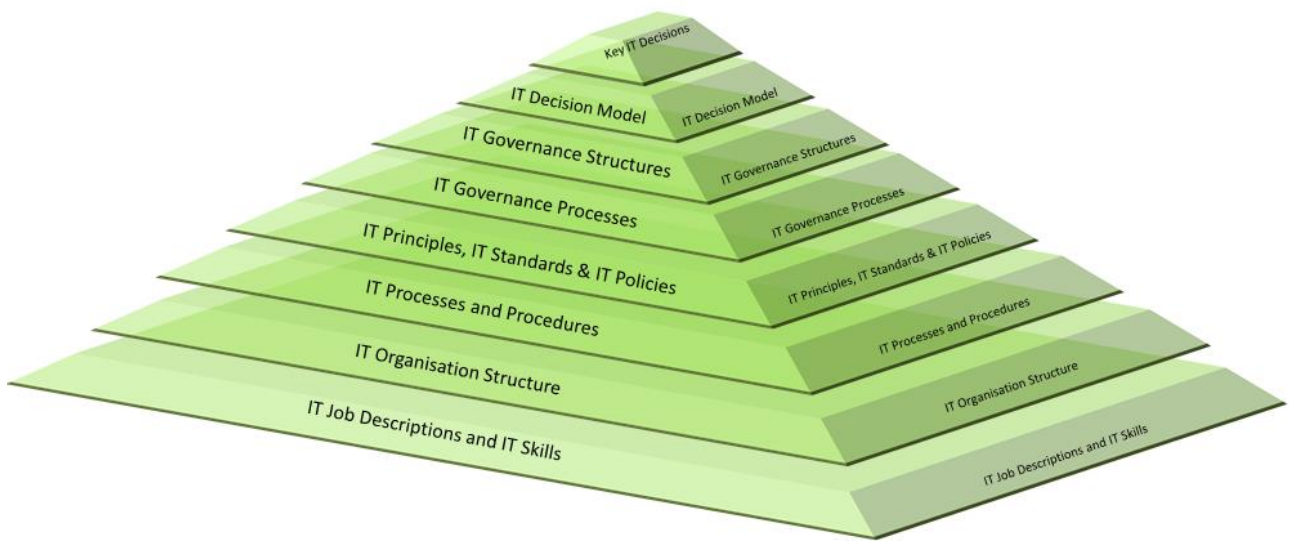
11.2 The implementation of Corporate Governance of ICT in the Municipality thus consists of the following layered approach:

11.2.1 This Municipal Corporate ICT Governance Framework Policy, which addresses the Corporate Governance of ICT layer at a strategic level.

11.2.2 Other best practice frameworks which will be adapted to give effect to the governance of the ICT operational environment within the Municipality.

## 12. ICT Governance Framework Components

The figure below illustrates the ICT Governance Framework that has been adopted by Senqu Municipality. Each of the components of the ICT Governance Framework is discussed in detail in the following sections.



**Figure 1: ICT Governance Framework Components**

## 12.1 Key ICT Policies

### 12.1.1 Introduction and Objective

The objective of this section is to identify and define the key ICT policies that typically need to be developed, approved and workshopped to all ICT End-Users within Senqu Municipality.

### 12.1.2 Implementation Guidance and Minimum Requirements

The following ICT policies are the supportive instruments and critical to be mentioned for the implementation of adopted by Senqu Municipality Municipal Corporate ICT Governance Framework Policy:

- 12.1.2.1 ICT Governance Charter
- 12.1.2.2 ICT Strategy.
- 12.1.2.3 ICT Internal Audit Plan
- 12.1.2.4 ICT Disaster Recovery Plan
- 12.1.2.5 ICT Management Policy
- 12.1.2.6 ICT Data Backup Recovery and Retention Policy
- 12.1.2.7 ICT Operating Systems Security Policy
- 12.1.2.8 ICT Security Controls Policy
- 12.1.2.9 ICT Security Policies
- 12.1.2.10 ICT SLA Management Policy
- 12.1.2.11 ICT User Access Management Policy
- 12.1.2.12 ICT Project and Portfolio Management Policy
- 12.1.2.13 ICT Risk Management Policy

#### **12.1.2.1 ICT Governance Charter**

Senqu Municipality has a dependency on ICT to enable its business processes. Due to the critical nature of ICT and the intellectual and other information resources that are exposed through technology channels, ICT governance now represents an essential component in ensuring the efficient and secure operation of the business. Chapter 5 of King V provides that the council, in exercising their duty of care, should ensure that prudent and reasonable steps have been taken with respect to ICT Governance. Chapter 5 sets out the following 7 principles:

- Council should be responsible for Information Technology (ICT) Governance.
- ICT should be aligned with the performance and sustainability objectives of the municipality.
  - Council should delegate to management the responsibility for the implementation of an ICT governance framework.
- Council should monitor and evaluate significant ICT investments and expenditure.
- ICT should form an integral part of the municipality's risk management.
- Council should ensure that information assets are managed effectively; and
- An audit committee should assist Council in carrying out its ICT responsibilities

#### **12.1.2.2 ICT Strategy**

Identification and positioning of strategic ICT initiatives and services which will best contribute to the achievement of the Municipality's strategic objectives and are agile and adaptive enough to support changes in the Municipality's strategy. Decisions in this domain include:

- Business relationship management.
- The approval of the ICT strategy.
- Ensuring that there is sufficient alignment with the Municipality strategy and that it sets the right direction for ICT within the Municipality.
- Implementation of the ICT strategy and monitoring of the outcomes and conflicting priorities.

#### **12.1.2.3 ICT Internal Audit Plan**

The purpose of this plan is to ensure that an approved Internal Audit schedule is in place to audit the ICT environment. The scope of work of the internal audit team is to determine whether the Municipality's ICT environment and governance processes, as designed and represented by management, are adequate and functioning in a manner to ensure that risks are appropriately identified and managed, ICT resources are used efficiently and adequately protected.

#### **12.1.2.4 ICT Disaster Recovery Plan**

It is essential to have a disaster recovery plan to provide for the recovery of those systems which support critical business functions and/or processes. The objective of this Disaster Recovery Plan is to provide a



structure and an action plan to be used in the timely recovery of the Municipality's critical applications' processing environment.

The main objective of this Plan is to recover the critical applications' processing environment within 48 hours following a disaster.

#### **12.1.2.5 ICT Management Policy**

Senqu Municipality requires an ICT management policy to provide a consistent management approach to ensure the Municipality's governance requirements are met.

The purpose of this policy is to give guidance on matters relating to ICT Management. This policy applies to all employees of Senqu Municipality and all parties that interact with the information and systems of the Municipality.

Defining ICT Structure that will address the following:

- The scope of ICT functions, roles, capabilities and decision-making rights must be defined within the ICT organisational structure.
- ICT service and support activities performed by third party service providers must be included in the ICT organisational structure.
- The ICT organisational structure must be aligned to the Municipality's overall organisational model.
- Roles and responsibilities for each ICT function must be identified within the ICT organisational structure. DRAFT Senqu Municipality ICT Management Policy Page 6 Resolution: 019/OCM/17 Approved 28 July 2017
- The adequacy and effectiveness of the ICT organisational structure must be reviewed on a regular basis.
- The ICT Manager must represent ICT at executive management level to report on the extent to which projects from the ICT strategy are being implemented and in general how technology opportunities are being exploited within the Municipality.
- Supporting management committees or structures that have a role in the decision-making process must be identified and included within the ICT decision model.
- ICT decisions must follow the decision-making model defined in the Municipality's ICT Charter.
- The ICT Steering Committee must be used as the forum for ICT decisions and must follow the decision and communication structure as defined in the ICT Charter.
- An approved Terms of Reference must exist for the ICT Steering Committee.

#### **12.1.2.6 ICT Data Backup Recovery and Retention Policy**

This document sets out Senqu Municipality's policy towards taking backups of its information assets, including their frequency, storage, retention, documentation, and restoration.

The purpose of the backup policy is to prevent the loss of data in the case of accidental deletion or corruption of data, system failure or disaster and to safeguard the information assets of Senqu Municipality by managing and securing backup and restoration processes and the media employed in the process.

The following strict conditions must be met as part of information security protection and its integrity protocols.

- Regardless of classification, the availability of all data must be maintained by means of periodic back-ups and recovery mechanisms.
- All data relating to applications, information and configuration must be backed up regularly and taken off-site to a secure location.

#### **12.1.2.7 ICT Operating Systems Security Policy**

As a government institution, Senqu Municipality must implement an IT Operating Systems Security Policy. Effective implementation of this policy will minimise the risk of unauthorised access to the Municipality's Operating Systems.

Senqu Municipality requires an IT Operating Systems Security Policy to ensure that consistent security controls are applied to minimise the risk of vulnerabilities on the network.

This document is to provide guidance for the Information Technology (IT) security controls that should be implemented for Senqu Municipality on the Windows operating system.

#### **12.1.2.8 ICT Security Controls Policy**

IT security is characterised as the preservation of the confidentiality, integrity and availability of information and associated assets. The IT Security Control Policy is intended to provide a common basis for developing organisational security standards and effective security management.

In order to promote a working environment that is conducive to teamwork and productivity, it is essential that all users understand their roles and responsibilities with regards to Information Technology (IT) security and adhere to the security requirements of Senqu Municipality. IT security is therefore characterised as the preservation of:

- Confidentiality – Ensuring that information is only accessible to those individuals who are duly authorised to have access to it.
- Integrity – Safeguarding the accuracy and completeness of information and processing methods.
- Availability – Ensuring that authorised users have access to information and associated assets as and when required.

#### **12.1.2.9 ICT Security Policies**

Information and information systems are critical and vitally important to the municipality. Without reliable information the municipality could be adversely affected, both financially and reputation wise. Therefore, this policy states the minimum requirements and the responsibility that all councilors, employees, temporaries, contractors and management must comply with in order to secure the municipality's information.

SENQU Municipality management has a duty to preserve, improve, and account for all information and information systems. They must additionally make sure that information assets are protected in a manner that is at least as secure as other organisations in the same industry handling the same type of information. To achieve this objective, annual reviews of the risks to SENQU Municipality's information assets will be conducted. Similarly, whenever a security incident or audit finding indicates that the security of information or information systems is insufficient, management must promptly take remedial action to reduce the municipality's exposure.

#### **12.1.2.10 ICT SLA Management Policy**

The IT suppliers for Senqu Municipality must be managed to ensure that they meet the Municipality's requirements. This is achieved by practising adequate performance and monitoring processes of IT suppliers and IT service providers.

This policy applies to all employees of the Municipality and all third parties that interact with the information and systems of Senqu Municipality.

#### **12.1.2.11 ICT User Access Management Policy**

As a government institution, Senqu Municipality must implement an IT User Access Management Policy to maintain an adequate level of security to protect the Municipality's data and information systems from unauthorised access and to ensure a secure and reliable operation of the Municipality's information systems.

The objective of this policy is to ensure the effective and efficient management of access to the municipality's information resources and systems and includes:

- Granting access after relevant management authorisation and an official request has been received.
- Removing access upon role change, service termination or contract expiry.
- Resetting of access on positive identification of the owner of the user ID as the requestor.
- Updating access as required after an official authorised request has been received.
- Regularly reviewing the granted access privileges of users to determine whether they are still valid and necessary.

#### **12.1.2.12 ICT Project and Portfolio Management Policy**

IT programmes and projects must be managed in a co-ordinated and structured manner to enable improvement on the quality and value of project deliverables and reduce the risk of unexpected delays and increased costs.

The purpose of this policy is to give guidance on matters relating to the planning, initiation and management of IT projects using formal project management techniques. In addition, an IT Project Portfolio must be managed in a co-ordinated and structured manner to enable improvement on the quality and value of project deliverables and reduce the risk of unexpected delays and increased costs.

This policy applies to all employees of Senqu Municipality and all parties that interact with the information and systems of the Municipality as well as to give guidance on matters relating to the planning, initiation and management of IT projects using formal project management techniques.

#### **12.1.2.13 ICT Risk Management Policy**

As a government institution, Senqu Municipality must implement and support risk management relating to information systems. This includes reducing IT related risk as well as integrating the management of IT-related risk with the Municipality's overall risk management strategy.

The purpose of this policy is to ensure that all IT risks are effectively and efficiently managed. This policy applies to all employees of Senqu Municipality and all parties that interact with the information and systems of the Municipality.

Risk Management Evacuation is comprising of:

- The level of IT-related risk that the municipality is willing to accept in pursuit of its objectives (risk appetite) must be determined.
- IT risk tolerance thresholds must be evaluated and approved based on the municipality's acceptable risk and opportunity levels.
- The IT environment must be subject to risk assessments and evaluation to ensure compliance with national standards and legislation.

## 12.2 ICT Decision Making Model

### 12.2.1 Introduction and Objective

The objective of this section is to determine which stakeholders need to be involved in each of the decision domains as well as to determine the role each stakeholder will play when a decision is to be made based on the types of key ICT decisions defined in section 12.1.

### 12.2.2 Implementation Guidance and Minimum Requirements

When developing the decision model for each decision category, the type of involvement that is required from each stakeholder must be documented. The various roles that a stakeholder could have when participating in decision making are as follows:

- 12.2.2.1 **Responsible** for a decision: The stakeholder making the decision to achieve the deliverable.
- 12.2.2.2 **Accountable** for a decision: The stakeholder ultimately answerable for the decision that has been made and the one who delegates the work to those responsible.
- 12.2.2.3 **Consulted** during a decision: Stakeholders whose opinions are sought when planning. These are typically subject matter experts and with whom there is two-way communication.
- 12.2.2.4 **Informed** about a decision: Stakeholders who are kept up to date on progress, often only on completion of the project or deliverable and with whom there is just one-way communication.

Senqu Municipality stakeholders involved in the ICT decision model are as follows:

- Municipal Manager
- SEM
- EXCO
- Audit and Performance Committees
- ICT Steering and Risk Management Committees
- Senqu Municipal Council
- CFO

- ICT Manager

The decision model adopted by Senqu Municipality is depicted in Table 1 overleaf.

**Table 1: ICT Decision Making Model**

ICT Decision Category	Formal Decision-Making Body	Council	EXCO	Municipal Manager	Senior Executive Management	Top Management	Audit Committee	Performance and Risk Committees	ICT Steering Committee	CFO	ICT Manager
ICT Governance, Risk and Compliance	Senior Executive Management/Risk Management/Audit Committee	C/I	C/I	A/R	C/R/I	C/I	C/I	C/I	C/R/I	A/R	A/R
ICT Strategy	Senior Executive Management	C/I	C/I	A/R	A/R	C/I	I	I	C/I	A/R	R
Application Management	Finance Management	I	I	I	R/C/I	C/I/A	I	I	C/I	R	R
Information Management	Senior Executive Management	R	R	A/R	A/R	A/R	I	I	C/I	A/R	A/R
Business and ICT Architecture	Finance Management	C/I	C/I	A	A/R	C/I	I	I	C/I	R	A/R
ICT Investments and Projects	Senior Executive Management	C/I	C/I	A	A/R	C/I	I	I	C/I/R	C/I/R	R
ICT Insourcing and Outsourcing	Senior Executive Management	C/I	C/I	A	A/R	A/R/I	I	I	C/I/R	C/I/R	
ICT Security	Finance Management	C/I	C/I	A	A/R	C/I/R	I	I	C/I/R	A/R	A/R
ICT Operations	Finance Management	I	C/I	I	I	I	I	I	C/I	A/R	A/R
General ICT Management and Administration	Finance Management and Finance Standing Committee	I	I	I	C/I	C/I	I	I	C/I	A/R	A/R
ICT Change Management	Finance Management	I	I	C/I	C/I	C/I	I	I	C/I/R	A/R	A/R

**Key:**

- R = Responsible
- A = Accountable
- C = Consulted
- I = Informed

---

## 12.3 ICT Governance Structures

### 12.3.1 Introduction and Objective

ICT governance structures establishes the strategic, operational, and technical decision-making process required to ensure ICT enables Senqu Municipality to excel in its mission. The objective is to establish decision making bodies or committees, membership of these committees, the responsibilities they will assume and how these bodies interact with each other.

#### 12.3.1.1 Implementation Guidance and Minimum Requirements

For each governance structure, it must be clearly documented what responsibilities the structure has, the composition of the structure as well as the relationship and interaction between other governance structures, frequency of meetings, communication lines and quorums to be able to make decisions.

#### 12.3.1.2 ICT Steering Committee

Senqu Municipality (Senqu) established an Information Communication Technology Steering Committee to be known as the Senqu ICT Steering Committee.

In these terms of reference Senqu ICT Steering Committee refers to Senqu Municipality (Senqu) Information Communication Technology Steering Committee.

The following constitutes the terms of reference of Senqu ICT Steering Committee.

#### 1. Purpose

The purpose of the Senqu ICT Steering Committee is to facilitate and oversee the development of the institutions Information Communication Technology systems and governance procedures in order to:

- Address the strategic information technology issues pertaining to the requirements of the Institution.
- Ensure the alignment of systems in order to comply with legislation and the ongoing needs of the municipality.
- Provide oversight for the Senqu Information Communication Technology section in terms of the overall governance procedures of the institution.
- Identify issues and needs within the institution and propose solutions to be investigated.
- Promote the development of the Senqu Information Communication Technology systems in line with the requirements of the institution.
- Approve a budget framework to be carried forward to the budget and finance committee for consideration

In pursuing of this purpose, the Senqu ICT Steering Committee will ensure that:

- Available resources are utilised as efficiently as possible

- Duplication of resources is minimised
- There is a coordinated approach to all municipal requirements
- Best value for money practices is implemented

## **2. Objective**

- Communicate the primary responsibilities and delegated authority of the ICT Steering Committee for the effective and efficient management of Information Communications Technology resources in order to facilitate the achievement of corporate objectives.
- To ensure compliance with the adopted Governance Framework and Standards.

## **3. Role of the IT Steering Committee**

- Place ICT on the Executive Management meeting agenda
- Strategic alignment of ICT with corporate objectives and goals
- Monitor the action plans emanating from ICT audits.
- Risk management in support of the strategic and business objectives
- Preparation of an official Code of Conduct that will be included with the appointment letter of all members Interpret policy for action
- Guide strategic decisions on ICT investment initiatives
- Approve internal control frameworks
- Delegate responsibility for implementing an ICT governance framework
- Determine and communicate levels of risk tolerance/appetite
- Assign accountability for the organizational changes needed for ICT to succeed.

## **4. Steering Committee: Terms of reference**

- Align ICT Strategic direction to business strategy
- High-level budgetary allocation
- ICT value measurement and reporting
- ICT policy direction and adoption
- Oversee Disaster Recovery plans & preparedness
- Oversee ICT Risk Framework
- Oversee internal control frameworks implementation
- Oversee compliance to legislation and Information security framework

## **5. Steering Committee: Responsibilities**

- Promoting acceptance of strategically selected projects,



- Achievement of municipal goals objectives,
- Ensure a clear scope and adherence to scope management procedures,
- Providing the required analysis to correctly provide the relevant resources,
- Contingency management
- Realization of expected benefits from speedy and effective decision making
- Providing relevant information to the decision-making authority.

## 6. Membership

The ICT Steering Committee (Steer-Com) comprises of senior staff members who are owners or users of ICT information systems within the institution. This committee will have the final authority in determining the strategic objectives of ICT in the municipality. All ICT investments are central to their decision making. The committee will have a quorum to ensure that key decisions that require their involvement are made in a timely manner.

Membership of the committee will comprise of the following:

### Permanent Members

- Chief Financial Officer (Chairperson)
- Secretariat
  - ICT Network Technician
- Corporate Services
  - Permanent – Manager: Stakeholder Engagement and Council Support
  - Alternate - Manager: Administration, Building Preservation & Fleet Management
- Community Services
  - Permanent - Manager: Waste Management Services
  - Alternate - Manager: Amenities, Community Services
- DTPS
  - Permanent - Manager: IPED, Development and Town Planning
  - Alternate - Manager: Governance and Compliance
- Finance
  - Permanent - Manager: Information Communication Technology
  - Alternate - Manager: Revenue
- Office of the Municipal Manager
  - Permanent - Manager: Strategic Support (Deputy Chairperson)
  - Alternate - Communications and Political Affairs Manager
- Technical Services
  - Permanent - Electro Technical Controller
  - Alternate – Manager: PMU

### Ad-hoc Members

The Municipal Manager and any Directors or Managers are welcome to attend the meetings.

The ICT Steering Committee is considered to be a subcommittee of top management. All items from the ICT Steering Committee may be recommended directly to top management for approval.

Any other representative from Senqu Municipality or of an institution or group that may be deemed to have a meaningful contribution to make may be co-opted to join the Senqu ICT Steering Committee at any time with the agreement of the members.

## **7. Meeting Frequency**

Ordinary ICT Steering Committee meetings are scheduled to be held once quarterly. Meetings can be held at regular intervals depending on the municipality ICT demands but not less than four times per year.

The venue for each meeting will be decided by the Chairperson and will take place at any venue suitable to a majority of the Senqu ICT Steering Committee members.

## **8. Chairperson**

The Chairperson of each meeting will be the CFO or the Deputy Chairperson in the absence of the Chairperson or a person delegated by the CFO.

All decisions shall be made if possible, by consensus. A simple majority vote shall only be used as a last resort.

## **9. Steering Committee Quorum**

The meeting will be considered to have quorum when

- The Chairperson/ Deputy Chairperson is present and
- 50% of the appointed members plus a Chairperson/Acting Chairperson
- In the event of a quorum not being present, but with written consent from the absent members, the meeting may continue.

## **10. Responsibilities of the Steering Committee Chairperson**

The chairperson is responsible for:

- Acting as a vocal and visible champion for the committee,
- Legitimizes the directives and delegation,
- Alignment of ICT to strategic objectives of municipality,
- Approves changes in scope,
- Approval and sign-off of deliverables,
- Ensuring that Steering Committee meetings are held as required by the governance framework.
- Efficient performance by the committee's secretariat.

#### **11. Responsibilities of ICT Steering Committee Members**

Individual members have the following responsibilities:

- Align ICT investments to their respective business objectives,
- Ensure the realisation of expected benefits,
- Engage with ICT for value optimization,
- Ownership of information security within respective business sphere,
- Resource allocation for systems impacting respective business goals,
- Feedback on user experience,
- Highlight business risk.

#### **12. Responsibilities of the Steering Committee Secretariat**

The Secretariat will be responsible for the following activities:

- Scheduling of meetings as per Chairperson's directive,
- Producing documentation and meeting minutes,
- Managing correspondence,
- Information management / dissemination and related tasks.

#### **13. Steering Committee Meeting Documentation**

The Secretariat will distribute meeting documents to members five business days in advance of a committee meeting. This package will include the following:

- Draft Agenda for upcoming meeting.
- Minutes of previous meeting including open action items and closed action items.
- Decision papers; and
- Any other documents/information to be considered at the meeting.

**Meeting packs and documentation will be distributed electronically as far as possible.**

#### **14. Document Library**

A record of each meeting will be kept by the Secretariat who remains responsible for the completeness of meeting documentation (ICT Steering Committee file). Master Files are kept at the Director Corporate Services' Office through Records Management - unit.

All minutes to be circulated as per the Senqu policy, but not less than 24 hours before the date of the next meeting.

All decisions taken by the ICT Steering Committee are considered to have been approved by the Top Management Structure and if required may be forwarded directly to the Standing

committee for further action.

Amendments to these Terms of Reference may be made at any time with the agreement of the committee.

**15. Steering Committee Document Library**

The Secretariat remains responsible for the completeness of meeting documentation (ICT Steering Committee file). Master Files are kept at the Director Corporate Services' Office through Records Management - unit.

**16. Adjustments AND Approval**

The ICT Steering Committee is to review recommended adjustments to these terms of reference at least once within every 12-month period. These terms of reference cannot be adjusted without approval of the Executive Management.

The ICT Charter is endorsed by the Chairperson of the ICT Steering Committee and approved by the Council of the Municipality.

An ICT Steering Committee must be established by Senqu Municipality and must take oversight responsibility for making decisions with regard to the following ICT decision categories:

- 12.3.1.2.1 ICT Governance, Risk and Compliance.
- 12.3.1.2.2 ICT Strategy.
- 12.3.1.2.3 Application Management.
- 12.3.1.2.4 Information.
- 12.3.1.2.5 Business and ICT Architecture.
- 12.3.1.2.6 ICT Investments and Projects.
- 12.3.1.2.7 ICT Sourcing.
- 12.3.1.2.8 ICT Security.
- 12.3.1.2.9 ICT Operations.
- 12.3.1.2.10 General ICT Management and Administration.
- 12.3.1.2.11 ICT Change Management.

The ICT Steering Committee will monitor the committee resolution register and make recommendations to the Senior Executive Management (SEM). The ICT Steering Committee functioning and effectiveness will be oversighted by Audit, Risk and Performance Committees.

## 12.4 ICT Governance Processes

### 12.4.1 Introduction and Objective

ICT Governance processes are required to be implemented to facilitate and enable the ICT Governance Framework on a day-to-day basis. The processes below will form part of the framework.

### 12.4.2 Implementation Guidance and Minimum Requirements

#### 12.4.2.1 Management of Exceptions

This is a documented and structured mechanism for stakeholders to state their case and request exceptions to defined policies, standards and principles. It also includes the activities that are followed to escalate requests that are deemed to be required but have been rejected.

Refer to Appendix A1 for details on the process flow.

#### 12.4.2.2 Management of Risk

ICT risk management is the process of identifying ICT risks, assessing these risks and taking steps to reduce risk to an acceptable level. Risk management is an essential function of the Municipality, and therefore ICT risk management must integrate with the Municipality's overall risk management process.

The objective of the risk management process is to allow ICT management to balance the benefits and costs of protective measures and to support the strategic objectives by adequately protecting all ICT assets that support the Municipality's strategic objectives.

Refer to Appendix A2 for details on the process flow.

#### 12.4.2.3 Agreement and Management of Service Levels

The main objective of the service level and agreement process is to enable the delivery of reliable, responsive, effective and efficient ICT services, that meets the Municipality's requirements as precisely as possible.

Service level agreements represent the internal contract between the ICT business unit and other business units. SLA's often result in improved behavior from business units – by exposing the ICT impact of their business requirements and requests for services, the business units have an improved understanding of the ICT environment, its resources and constraints. The SLA is usually based on a Service Catalogue (SC) which lists available ICT services, alternative quality levels and related costs. The negotiation of the SLA is an important governance process since it leads to

increased business/ICT alignment through greater clarity on Municipal requirements. It also leads to improved sourcing decisions. Once requirements are explicitly stated in a detailed form, comparison can be made between internal service provisioning and outsourced options.

Refer to Appendix A3 for details on the process flow.

## 12.5 ICT Principles, ICT Practices, ICT Standards and ICT Policies

### 12.5.1 ICT Principles

#### 12.5.1.1 Introduction and Objective

Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which the Municipality sets about fulfilling its mission.

#### 12.5.1.2 Implementation Guidance and Minimum Requirements

Below are the guiding Corporate Governance of ICT Principles that have been adopted by Senqu Municipality. These principles are based on the principles described in the Municipal Corporate ICT Governance Framework Policy.

**Table 2: Municipal Corporate Governance of ICT Principles**

No.	Principle	Description
1	<b>Political Mandate</b> The Governance of ICT must enable the municipality's political mandate.	The Municipal Council must ensure that Corporate Governance of ICT achieves the service delivery mandate of the municipality.
2	<b>Strategic Mandate -</b> The Governance of ICT must enable the municipality's strategic mandate.	The Municipal Manager must ensure that Corporate Governance of ICT serves as an enabler to the municipality's strategic plans.
3	<b>Corporate Governance of ICT</b> The Municipal Manager is responsible for the Corporate Governance of ICT.	The Municipal Manager must create an enabling environment in respect of the Corporate Governance of ICT within the applicable legislative and regulatory landscape and information security context.
4	<b>ICT Strategic Alignment</b> ICT service delivery must be aligned with the strategic goals of the municipality.	Management must ensure that ICT service delivery is aligned with the municipal strategic goals and that the administration accounts for current and future capabilities of ICT. ICT must ensure that ICT is fit for purpose at the correct service levels and quality for both current and future Municipal needs are met.
5	<b>Significant ICT Expenditure</b> Management must monitor and evaluate significant ICT expenditure.	Management must monitor and evaluate major ICT expenditure, ensure that ICT expenditure is made for valid Municipal enabling reasons and monitor and manage the benefits, opportunities, costs and risks resulting from this expenditure, while ensuring that information assets are adequately managed.
6	<b>Risk Management and Assurance</b> Management must ensure that ICT risks are managed and that the ICT function is audited.	Management must ensure that ICT risks are managed within the municipal risk management practice. ICT must also ensure that the ICT function is audited as part of the municipal audit plan.

<b>7</b>	<b>Organisational Behaviour</b> Management must ensure that ICT service delivery is sensitive to organisational behaviour/culture.	Management must ensure that the use of ICT demonstrates the understanding of and respect for organisational behaviour/culture.
----------	---	--

## 12.5.2 ICT Practices

### 12.5.2.1 Introduction and Objective

The following practices, outlined in Table 3 below, have been assigned to specific designated municipal structures and officials in order to achieve the objectives and principles contained in this Municipal Corporate ICT Governance Framework Policy:

**Table 3: Municipal Corporate ICT Governance Framework Policy Practices**

No.	Practice Description
1.	<p><b>The Municipal Council must:</b></p> <p>Provide political leadership and strategic direction through:</p> <ol style="list-style-type: none"> <li>a. Determining policy and providing oversight.</li> <li>b. Take an interest in the Corporate Governance of ICT to the extent necessary to ensure that a properly established and functioning Corporate Governance of ICT system is in place in the municipality to leverage ICT as an enabler of the municipal IDP.</li> <li>c. Assist the Municipal Manager to deal with intergovernmental, political and other ICT-related Municipal issues beyond their direct control and influence.</li> <li>d. Ensure that the municipality's organisational structure makes provision for the Corporate Governance of ICT.</li> </ol>
2.	<p><b>The Municipal Manager must:</b></p> <ol style="list-style-type: none"> <li>a. Provide strategic leadership and management of ICT.</li> <li>b. Ensure alignment of the ICT strategic plan with the municipal IDP.</li> <li>c. Ensure that the Corporate Governance of ICT is placed on the municipality's strategic agenda.</li> <li>d. Ensure that the Corporate Governance of ICT Policy, Charter and related policies for the institutionalisation of the Corporate Governance of ICT are developed and implemented by management.</li> <li>e. Determine the delegation of authority, personal responsibilities and accountability to Management with regards to the Corporate Governance of ICT.</li> <li>f. Ensure the realisation of municipality-wide value through ICT service delivery and management of Municipal and ICT-related risks.</li> </ol>



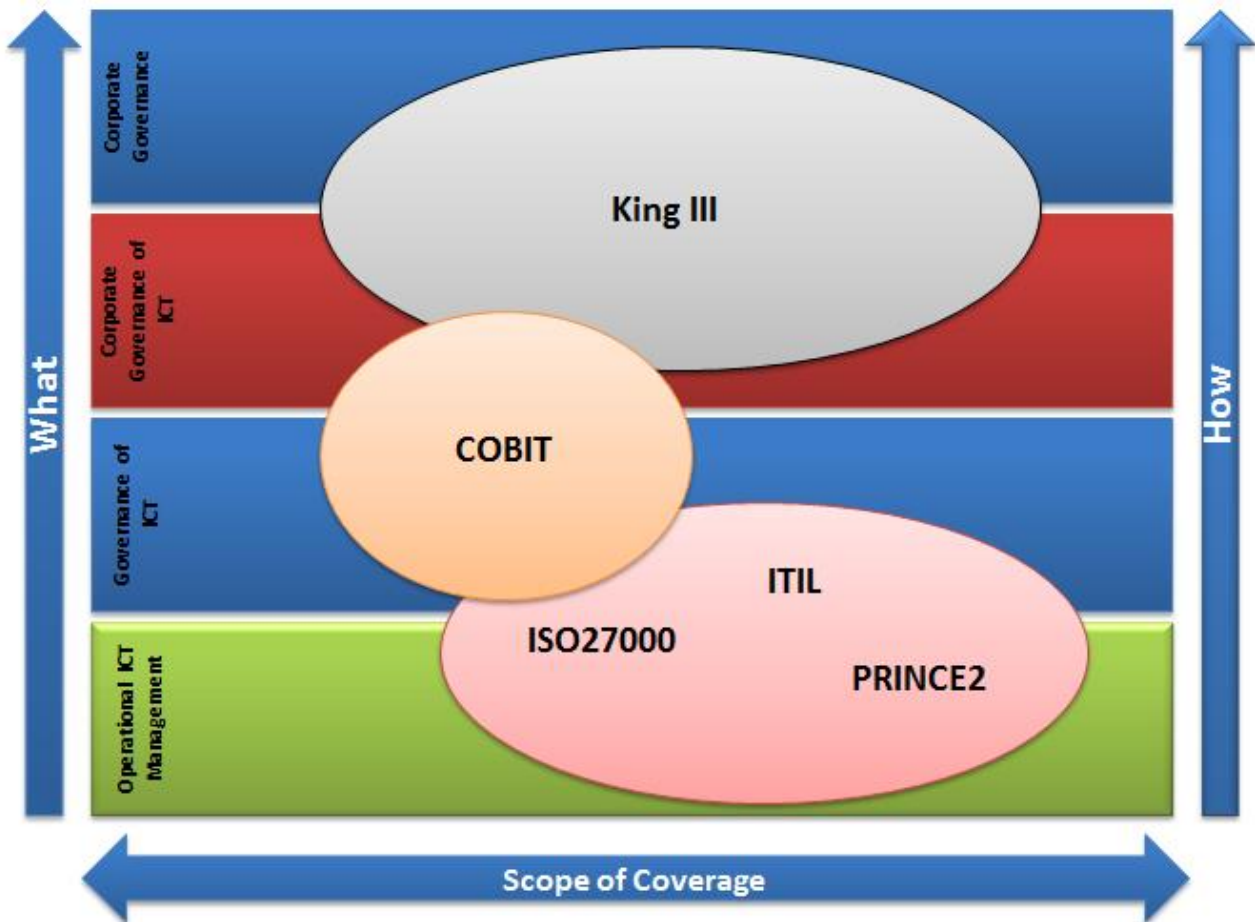
No.	Practice Description
	<ul style="list-style-type: none"> <li>g. Ensure that appropriate ICT capability and capacity are provided and a suitably qualified and experienced Governance Champion is designated.</li> <li>h. Ensure that appropriate ICT capacity and capability are provided and that a designated official at a Management level takes accountability for the Management of ICT in the municipality.</li> <li>i. Ensure the monitoring and evaluation of the effectiveness of the Corporate Governance of ICT system through the ICT steering committee.</li> </ul>
3.	<p><b>The Municipal ICT Steering Committee and the Audit and Performance Committee must:</b></p> <ul style="list-style-type: none"> <li>a. Assist the Municipal Manager in carrying out his/her Corporate Governance of ICT accountabilities and responsibilities.</li> </ul>
4.	<p><b>Management must ensure:</b></p> <ul style="list-style-type: none"> <li>a. ICT strategic goals are aligned with the Municipality's strategic goals and support the municipal processes.</li> <li>b. Municipal-related ICT strategic goals are cascaded throughout the municipality for implementation and are reported on.</li> </ul>

### 12.5.3 ICT Standards

#### 12.5.3.1 Introduction and Objective

A standard is defined as a document established by consensus and approved by a recognised body that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

The figure overleaf depicts the different layers of governance and the interrelationship between the different Frameworks and Standards adopted by the Municipality. All of the frameworks reflected in the figure below are generally accepted frameworks. King V is the corporate governance standard adopted by most entities in South Africa and the other standards like ISO, ICTIL, PRINCE2 and COBICT are internationally recognised frameworks and standards operating at different levels within the ICT Governance Framework.



**Figure 3: Interrelation between adopted Codes, Frameworks and Standards**

**12.5.3.2 Implementation Guidance and Minimum Requirements**

Figure 3 above reflects the frameworks, standards and codes that have been used to develop the ICT Governance Framework. The standards, frameworks and codes reflected in Figure 3 are internationally recognised or generally accepted standards. Table 4 overleaf provides a general description of each standard or framework which has been adopted by Senqu Municipality.

Table 4: ICT Frameworks and Standards

Framework/Standard	Description
<b>King V</b>	King V Code is a Code of Good Governance emphasising corporate leadership, business sustainability and corporate citizenship. The King V Code is the most commonly accepted corporate governance framework in South Africa and is also valid for the public sector.
<b>COBICT</b>	COBICT is an internationally accepted process framework for the implementation of the governance of ICT. COBICT fully supports the principles of the King V Code and the ISO 38500 standard on the corporate governance of ICT. Principle 5.1.3 of the King V Report on Governance recommends that an ICT internal control framework be adopted and implemented.
<b>ISO/IEC 27002</b>	ISO/IEC 27002 is a code of practice for information security management. It can be used by any organisation that needs to establish a comprehensive information security management program or improve its current information security practices. ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS).
<b>ITIL</b>	The Information Technology Infrastructure Library (ITIL) is a set of practices for ICT service management (ITSM) that focuses on aligning ICT services with the needs of business. It provides a practical framework for identifying, planning, delivering and supporting ICT services to the business. It will provide guidance to the Municipality on how to use ICT as a tool to facilitate business change, transformation and growth.
<b>PRINCE2</b>	PRINCE2 (an acronym for PROjects IN Controlled Environments) is a de facto process-based method for effective project management. Used extensively by the UK Government, PRINCE2 is also widely recognised and used in the private sector, both in the UK and internationally. The PRINCE2 method is in the public domain and offers non-proprietary best practice guidance on project management. PRINCE2 will be adopted and used for managing projects within the Municipality.

#### 12.5.4 ICT Policies

##### 12.5.4.1 Introduction and Objective

Policies are approved at the highest level of the Municipality and are designed to remain in effect regardless of changes in people, technology or the mission of the Municipality. The need for policies is driven by the Municipality's objectives, resource requirements, organisational risks, rules and legislation and the maturity level of the Municipality. It also provides guidance for standards, processes and procedures, controls and structures.

#### **12.5.4.2 Implementation Guidance and Minimum Requirements**

The following ICT policies will be adopted by the Municipality:

- 12.5.4.2.1 Municipal Corporate ICT Governance Framework Policy
- 12.5.4.2.2 ICT Governance Charter
- 12.5.4.2.3 ICT Risk Management Policy
- 12.5.4.2.4 ICT Internal Audit Plan
- 12.5.4.2.5 ICT Management Policy
- 12.5.4.2.6 ICT Project and Portfolio Management Policy
- 12.5.4.2.7 ICT Disaster Recovery Plan
- 12.5.4.2.8 Data Backup and Recovery Policy
- 12.5.4.2.9 ICT Service Level Agreement Management Policy
- 12.5.4.2.10 ICT User Access Management Policy
- 12.5.4.2.11 ICT Security Controls Policy
- 12.5.4.2.12 ICT Operating Systems Security Policy

## **12.6 ICT Processes and Procedures**

### **12.6.1 Introduction and Objective**

Process: A sequence or order of activities that also outlines the different decision points and functions responsible. Processes are cross-functional and define what is done and by whom.

Procedures: Procedures define how certain activities are performed within a process.

### **12.6.2 Implementation Guidance and Minimum Requirements**

Processes are often depicted in diagrammatical form such as a decision tree or flowchart where the work performed is split into logical interrelated steps or “activities”. Processes must always have a “trigger” or start event and a “terminator” or end event that achieves a specific result.

Procedures are typically documented in a step-by-step order with detailed descriptions of how the work is to be performed and who is responsible for performing the work.

Senqu Municipality must design processes and procedures that are in-line with recognised standards.

The advantage of written processes and procedures will ensure that the Municipality’s outcomes are consistent and repeatable. In addition, written documentation increases the Municipality’s knowledge base.

---

## 12.7 ICT Organisational Structure

### 12.7.1 Introduction and Objective

The objectives of establishing an ICT organisational structure are as follows:

- 12.7.1.1 Alignment to new strategic directions of the Municipality.
- 12.7.1.2 Solve problems resulting from structure inefficiencies.
- 12.7.1.3 Eliminate job conflicts.
- 12.7.1.4 Clarify uncertainty regarding the hierarchy and distribution of work and responsibilities.
- 12.7.1.5 Alignment of the municipality systems to the new emerging technologies of the 4<sup>th</sup> Industrial Revolution Technologies

### 12.7.2 Implementation Guidance and Minimum Requirements

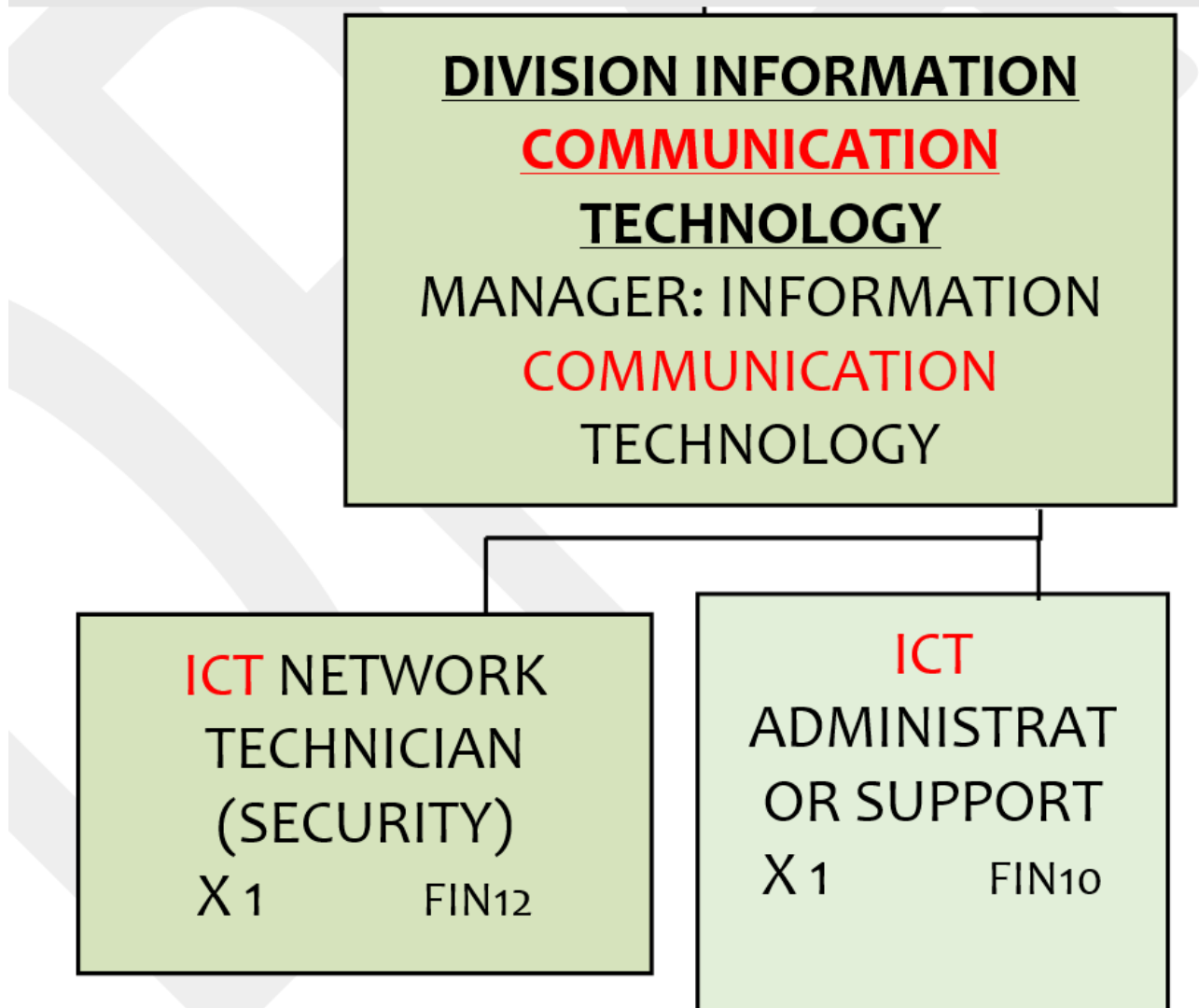
An internal and external ICT organisational structure must be established so that it reflects business needs. In addition, a process must be put in place for periodically reviewing the ICT organisational structure to adjust staffing requirements and sourcing strategies to meet expected Municipal objectives and changing circumstances.

Below are guidelines when designing and reviewing ICT organisational structures:

- 12.7.2.1 Accountability of activities must be placed where 'means' and 'interest' come together and as low as possible in the ICT organisation.
- 12.7.2.2 The ICT organisation structure must be as simple as possible to ensure fast decision-making, improved career planning, simplified ICT processes and to prevent bureaucracy and a silo mentality.
- 12.7.2.3 The ICT organisation structure must be appropriate to the size and complexity of the overall Municipality.
- 12.7.2.4 Unnecessary duplication in functions and job roles must be avoided to ensure uncertainty is not created with regards to roles and responsibilities
- 12.7.2.5 The ICT organisation structure must facilitate knowledge transfer and learning between team members.

The figure below illustrates Senqu Municipality’s current ICT organisational structure.

**Figure 4: Senqu Municipality’s ICT Organisational Structure**



**12.8 ICT Job Descriptions and ICT Skills**

**12.8.1 Introduction and Objective**

The objective of a job description is to explain the primary role of the position. Job descriptions provide a listing of the specific tasks and duties that the person in the job is responsible for completing. In addition, a job description clarifies the roles and relationships associated with the position.

## 12.8.2 Implementation Guidance and Minimum Requirements

### 12.8.2.1 Skills Requirements for Good ICT Governance

The following list as described by the South African Local Government Association (SALGA) gives an indication of the type and level of expertise of ICT skills that is required to move towards and manage a functional ICT Governance Framework.

**Table 5: High Level ICT Skill Requirements**

Skill	General Description
<b>Information Management</b>	The overall management of information, as a fundamental Municipal resource, to ensure that the information needs of the Municipality is met.
<b>Risk Management</b>	The planning and implementation of organisation-wide processes and procedures for the management of operational risk.
<b>Information Security</b>	The management of and provision of expert advice on, the selection, design, justification, implementation and operation of information security controls and management strategies to maintain the confidentiality, integrity, availability, accountability and relevant compliance of information systems.
<b>Security Administration</b>	The authorisation and monitoring of access to ICT facilities or infrastructure in accordance with established Municipal policies. Includes the investigation of unauthorised access, compliance with data protection and performance of other administrative duties relating to security management.
<b>Information Assurance</b>	The protection of systems and information in storage, processing, or transit from unauthorised access or modification. Denial of service to unauthorised users; or the provision of service to authorised users.
<b>Systems Architecture</b>	The specification of systems architectures, identifying the components needed to meet the present and future requirements, both functional and non-functional (such as security) of the Municipality as a whole and the interrelationships between these components.
<b>Continuity Management</b>	The provision of service continuity planning and support. This includes the identification of information systems that support critical Municipal processes, the assessment of risks to those systems' availability, integrity and confidentiality and the coordination of planning, designing, testing and maintenance procedures and contingency plans to address exposures and maintain agreed levels of continuity.
<b>Network Design</b>	The production of network designs and design policies, strategies, architectures and documentation, covering voice, data, text, e-mail, facsimile and image, to support Municipal requirements and strategy.
<b>Network Operations</b>	The day-to-day operation and maintenance of networked systems to ensure that the communication needs of the Municipality are met.
<b>Programming/Software Development</b>	The design, creation, testing and documenting of new and amended programs from supplied specifications in accordance with agreed standards.



Skill	General Description
<b>Web Site Specialism</b>	The design, creation, testing, implementation and support of new and amended collections of pages of information on the world wide web or an intranet or extranet.
<b>Project Management</b>	The management of projects, typically (but not exclusively) involving the development and implementation of Municipal processes to meet identified Municipal needs, acquiring and utilising the necessary resources and skills, within agreed parameters of cost, timescales and quality.
<b>Configuration Management</b>	The systematic management of information relating to the documentation, software, hardware and firmware assets of the organisation. This will involve identification and appropriate specification of all configuration items (CIs). Required information will relate to storage, access, problem reporting and change control of CIs.
<b>Change Management</b>	The management of all changes to the components of a live infrastructure, from requests for change (RFC) through to implementation and review, to support the continued availability, effectiveness and safety of the infrastructure.
<b>Capacity Management</b>	The management of the capability and functionality of hardware, software and network components to meet current and predicted needs in a cost-effective manner.
<b>Availability Management</b>	The overall control and management of services and their availability to ensure that all services meet all of their agreed availability targets.
<b>Financial Management for ICT</b>	The overall financial management, control and stewardship of the ICT assets and resources used in the provision of ICT services, ensuring that all governance, legal and regulatory requirements are complied with.
<b>Management and Operations</b>	The management and operation of the ICT infrastructure (typically hardware, software and communications) and the resources required to plan for, develop, deliver and support properly engineered ICT services and products to meet the needs of a business.

## 12.9 ICT Governance Communication

The communication mechanism that will be used to communicate ICT decisions to the various governance structures in place at the Municipality is as follows:

- 12.9.1 The ICT Steering Committee will have a direct communication line the Senior Executive Management and will communicate decisions taken in the following domains:

- 12.9.1.1 ICT Governance, Risk and Compliance.
- 12.9.1.2 ICT Strategy.
- 12.9.1.3 Application Management.
- 12.9.1.4 Information.
- 12.9.1.5 Business and ICT Architecture Planning.
- 12.9.1.6 ICT Investments and Projects.
- 12.9.1.7 ICT Sourcing.
- 12.9.1.8 ICT Security.
- 12.9.1.9 ICT Operations.
- 12.9.1.10 General ICT Management and Administration.
- 12.9.1.11 ICT Change Management.

12.9.2 The ICT Steering Committee will also have an indirect communication line to the Audit and Performance Committee and will communicate decisions taken regarding ICT Risk and Compliance.

### **13. Policy Violations**

13.1 Violations of this policy may result in disciplinary action, up to and including dismissal for employees, a termination of employment relations in the case of contractors or consultants, dismissal for interns, or suspension.

### **14. Policy Review**

14.1 This policy is subject to annual review or whenever it is deemed necessary by Senqu Municipality of, to ensure that it is aligned to prevailing resolutions, regulations and market conditions.

### **15. Publishing the Policy**

15.1 The policy shall be made available and accessible to all employees through manuals/hard copies.

## 16. Senqu Municipality Approval and Sign-Off

Date of Approval by Council:

Resolution Number:

---

**MUNICIPAL MANAGER**

---

**DATE**

### RECOMMENDATION

That the report be noted,

That the Municipal Corporate Governance Information Communications Technology (MCGICT) Policy be approved by Council.

Appendix A: ICT Governance Processes

A1: Management of Exceptions

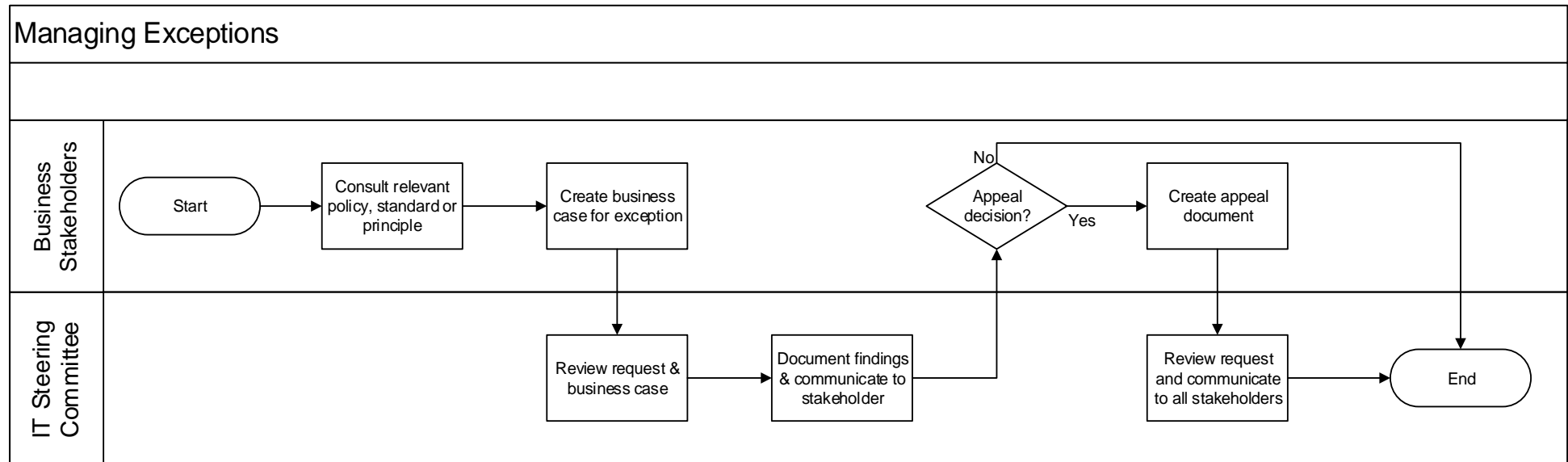


Figure 5: Management of Exceptions

A2: Management of Risk

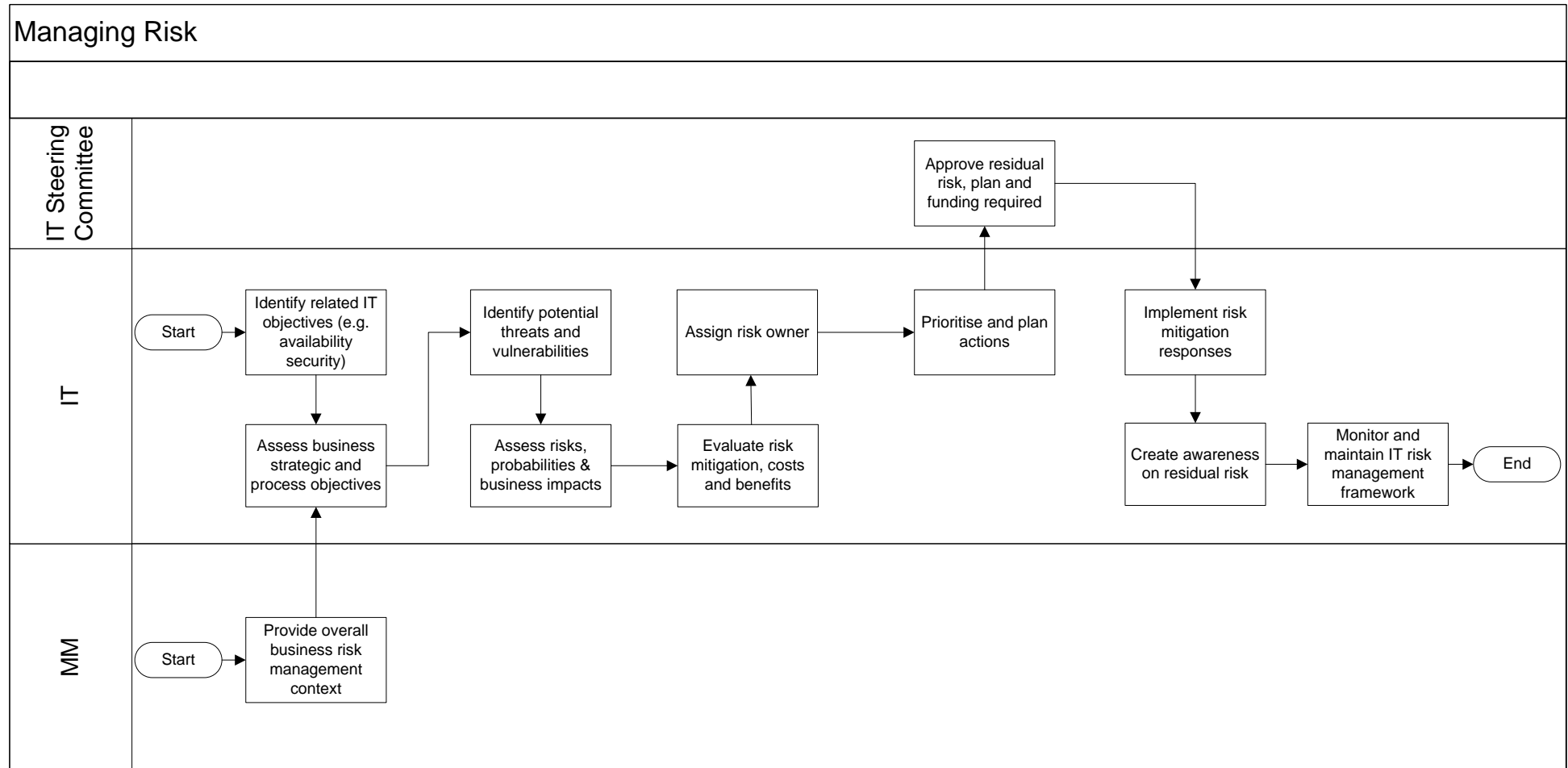
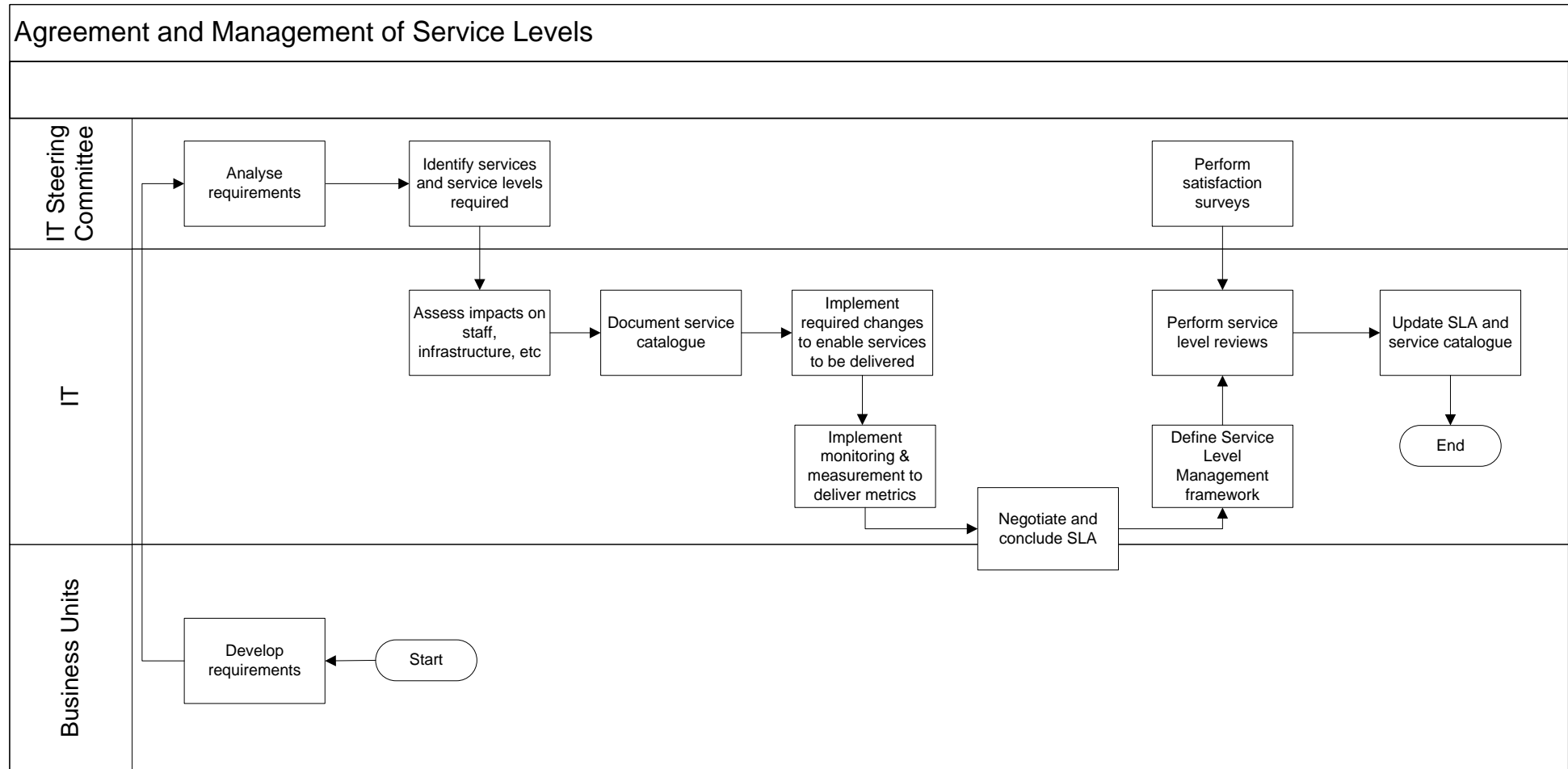


Figure 6: Management of Risk

A3: Agreement and Management of Service Levels



**Figure 7: Agreement and Management of Service Levels**